

QP Code : **MV-20289**

(3 Hours)

[Total Marks : 100

- N. B. : (1) Question No. 1 is compulsory.
(2) Attempt **any four** questions out of remaining **six** questions.
(3) Assume data if required and state it clearly.

1. (a) What are the different security goals? 5
(b) What is Keyless Transposition Cipher? Give any example of rail fence cipher. 5
(c) What are the different parameters used to measure the accuracy of biometric techniques? Also write the application of Biometric. 5
(d) What are the various types of IP Spoofing? 5
2. (a) Explain the TCP/IP Vulnerabilities at each layer. 10
(b) What are the typical characteristics of enterprise wide networks? Explain its different Router Vulnerabilities and Firewall Vulnerabilities. 10
3. (a) Explain A5/1 algorithm with an example. 10
(b) What are Passive and Active attacks? Categorize these attacks and explain one example of each. 10
4. (a) What is SHA-1? Explain different steps of working of SHA-1. 10
(b) What are the different methods of Malware (Malicious code) Detection? Explain with their advantages and disadvantages. 10
5. (a) What is Bell-La Padula? How Bell-La Padula model works? 10
(b) Explain different methods used to Commit a Session Hijack and methods to prevent Session Hijacking. 10
6. (a) Why Secure Socket Layer (SSL) is needed? What are the different features SSL provides? Explain how SSL works? 10
(b) How does Kerberos work? Explain with example. 10
7. Write short notes on the following:
(i) Multiple DES 10
(ii) Software Reverse Engineering (SRE) and prevention of SRE. 10